Remarks

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1-10, and 22 are currently pending;
- Claims 11-21 are withdrawn;
- Claims 1, 5, 7, 9 and 22 are amended herein; and
- Claims 23-31 are new claims.

[0003] Support for the amendments to claims 1, 5, 7, 9 and 22 are found in the specification at least at paragraph 10 of page 4; and paragraph 10 of page 12.

Cited Documents

[0004] The following documents have been applied to reject one or more claims of the application:

- Carter: Stephen Carter et al., U.S. Patent No. 6,601,171 B1 (Carter);
- Murakami: Takeo Murakami, U.S. Patent No. 5,845,082 (Murakami);
- Ault: Michael Bradford Ault, U.S. Patent No. 5,918,228 (Ault); and
- Kao: I-Lung Kao, U.S. Patent No. 7,451,147 B1 (Kao).

Overview of the Application

[0005] The Application relates to a secured distributed impersonation, such as can be used within batch systems (e.g., batch message transaction systems). In one embodiment, a method includes sending a request for network account credentials from an originating account associated with an unpublished object, to a dispatch associated with a published object. In one embodiment, both the unpublished and the published objects can each be a message queue. The request is sent specifically to the published object, and identifies the unpublished object. The originating account can be at a local computer, for example, within a system of which the dispatch is also a part. The network account credentials can be, for example, the account credentials that the originating account needs to properly perform a job that has been assigned to it.

[0006] The dispatch authenticates the originating account. Upon successful authentication, the network account credentials are sent to the originating account. In one embodiment, these account credentials are included in data that is generically referred to as non-restrictive and non-limited emblem. The emblem in one embodiment can be a secure manner by which the credentials are transmitted. For example, the emblem can be a token, as known within the art. The emblem is specifically sent to the unpublished object associated within the originating account, as identified in the initial request. The network account for which the originating account requested credentials can be a batch account of the dispatch itself, in one embodiment, while in another embodiment it can be an agent account onto which the dispatch proxy logs. In either case, the dispatch has the network account remoted back to the originating account. Furthermore, the network account can be any of a number of agent accounts, such that

any of the agent accounts may be remoted back to the originating account as the network account. Thus, the request for a network account may be a request for the credentials of a particular agent account, or for the credentials of any of a group of agent accounts.

Overview of Carter

[0007] Carter teaches a system and methods for delegating rights in a distributed computer system from a principal to one or more deputies. The deputies have identities separate from the principal. This allows the deputies to persist after the principal logs off the system, and permits deputization across boundaries imposed by namespaces and particular network protocols. A deputy may also delegate rights to additional deputies. Deputization is accomplished using certificates, credentials, public and private keys, process creation, and other tools and techniques.

Overview of Murakami

[0008] Murakami teaches an invention that provides a node apparatus and a storage apparatus for use with a distributed system and a recovery method for a resource managing server for a distributed system, which are improved in that the load to a server upon recovery of the server is reduced and the memory area of the server can be utilized effectively. The node apparatus is used with a distributed system which includes a plurality of node apparatus each including one or both of a client and a resource managing server and a storage apparatus for storing checkpoints and wherein the plurality of node apparatus and the server are interconnected by way of a network. The node apparatus at least includes a client, and includes a checkpoint taking unit for allowing, in ordinary operation of the distributed system, the client provided in the node

apparatus to take a checkpoint regarding a resource managed by the server, and a unit for storing the checkpoint taken by the checkpoint taking unit in the ordinary operation of the distributed system into the storage apparatus.

Overview of Ault

[0009] Ault teaches (enabling) continuous access to Web documents stored in a secure distributed file system (Ault, col. 1, lines 9-11). "A session manager is used to perform a proxy login to a security service on behalf of a Web server. Persistent operation of the session manager is ensured by periodically spawning new instances of the session manager process." *See Abstract of Ault*.

Overview of Kao

[0010] Kao describes a method in a data processing system for providing security to target passwords in a global sign on system centralized database. In a preferred embodiment, a target password is received by the global sign on system. The target password is encrypted in a user selected encryption manner to create an encrypted password. The encrypted password and an indication of encryption manner chosen is then stored in the centralized database.

Claims 1-5, 8, 9 and 22 stand rejected under 35 U.S.C. § 103(*a*) as allegedly being anticipated by Carter in view of Murakami, and Ault

[0011] Claims 1-5, 8, 9 and 22 stand rejected under 35 U.S.C. § 103(*a*) as allegedly being anticipated by Carter in view of Murakami, and Ault. Applicant respectfully traverses the rejection.

Independent Claim 1

[0012] Applicant submits that Carter in view of Murakami, and Ault does not teach Claim 1, because the references do not suggest, at least, the following features of Claim 1, as amended (with emphasis added):

> **assigning a job by a dispatch to an originating account**, the originating account not having adequate resources to accomplish the job
>
> sending a request for network account credentials from the originating account to the dispatch that is associated with a published object, the network account credentials include the resources to complete the job, the request directed to the published object includes an identification of an unpublished object associated with the originating account, the published object is accessible by an account without prior identification of the published object and the unpublished object is accessible by the account when the account is previously informed about the identification of the unpublished object

[0013] In rejecting Claim 1, the Office cites Carter (col. 7, line 38 to col. 8 line 16; col. 8, lines 30-67) in view of Murakami (Col. 1, lines 59-67), and Ault (col. 10, lines 3-21). The cited portions of Carter state:

> FIG. 2 illustrates generally the flow of data in a distributed computing system such as the system **100** during a deputization according to the invention. A user 200 wishes to be authenticated to a distributed deputization point 202 in

> order to delegate rights to one or more deputies. The user 200 first logs into the system **100** by exchanging login information 204 with a server 106. The server 106 will act as a principal node 206, that is, as a node 206 which represents a principal (one who delegates rights). The login information 204 exchange may be automatic if the user 200 is already logged into a client **110** that communicates with the principal node 206, or it may be done expressly at the user's request

[0014] Claim 1 recites "*assigning a job by a dispatch to an originating account.*" In contrast, Carter teaches a distributed computing system that delegates rights from a principal to one or more deputies. The one or more deputies have identities that are separate from the principal; however, the one or more deputies "may also delegate rights to additional deputies." *See Abstract of Carter.* Carter teaches a distributed deputization point (e.g., distributed deputization point 202) that authenticates a deputy credential request (e.g., deputy credential request 220) from the principal. After authentication, the principal may or may not be "authorized to create deputies." *See col. 8, lines 20-40 of Carter.* To this end, the distributed deputization point 202 teaches **the authorization of creating deputies** by the principal; however, the distributed deputization point 202 fails to teach or suggest "**assigning a job** by a dispatch to an originating account" as recited in Applicant's amended Claim 1.

[0015] In addition, Claim 1 further recites "*the request directed to the published object includes an identification of an unpublished object associated with the originating account, the published object is accessible by an account without prior identification of the published object and the unpublished object is accessible by the account when the account is previously informed about the identification of the unpublished object.*" In contrast, Carter teaches a system (e.g., system 100) where a principal can be granted with a deputy certificate "to deputize individual functions, agents, and/or other entities as

deputies." "Any access point in any network in the system 100 which can authenticate the deputy certificate can then authenticate the deputy to permit access to network resources in accordance with the rights and permissions granted in the deputy certificate." *See col. 9, lines 2-7 of Carter*. In other words, the request for the network in the system 100 (through the access point) can be permitted "in accordance with the rights and permissions granted in the deputy certificate;" however, Carter fails to teach "the request directed to the published object" as recited in Applicant's amended Claim 1.

[0016] In page 3, second paragraph of the Office Action (i.e., Aug. 11, 2009), the Examiner admits that "*Carter et al. fails explicitly to disclose that the request for credentials is for use in completing an assigned job*;" however, the Examiner cites Murakami (col. 1, lines 59-67) as allegedly teaching "*the request for credentials is for use in completing an assigned job*." The Applicant respectfully traverses this rejection.

[0017] The cited portions of Murakami state:

> in particular, when a client wants to use a resource managed by the server, the client first requests acquisition of a token of the resource, and after the client succeeds in acquisition of the token, it performs its job using the resource such as a file managed by the server. Thereafter, when the use of the resource is completed, the client returns the token to the server. Consequently, the same resource managed by the server is prevented from being used at a time by a plurality of clients

[0018] Claim 1 recites "*assigning a job by a dispatch to an originating account… the network account credentials include the resources to complete the job.*" In contrast, Murakami teaches providing "node apparatus and a storage apparatus for use with a distributed system and a recovery method for a resource managing server for a distributed system." *See Abstract of Murakami*. In particular, when a client wants to

use a resource managed by a server, the client first requests acquisition of a token of the resource, and after the client succeeds in acquisition of the token, the client performs its job using the resource, returning the token when the use of the resource is completed. The server managing the resource ensures that the resource is not used by plurality of clients at the same time. *See col. 1, lines 59-67 of Murakami.* To this end, Murakami teaches the use of the resource by the client after acquisition of the token; however, Murakami fails to teach "*assigning a job by a dispatch to an originating account"* as recited in Applicant's amended Claim 1. In addition, Murakami fails to discuss published and unpublished objects as described in Applicant's amended Claim 1.

[0019] Similarly, Ault fails to compensate the above-discussed deficiencies of Carter and Murakami. Ault teaches (enabling) continuous access to Web documents stored in a secure distributed file system (Ault, col. 1, lines 9-11). "A session manager is used to perform a proxy login to a security service on behalf of a Web server. Persistent operation of the session manager is ensured by periodically spawning new instances of the session manager process." *See Abstract of Ault*. To this end, Ault fails to teach or suggest "*assigning a job by a dispatch to an originating account"* as recited in Applicant's amended Claim 1.

[0020] Consequently, Carter in view of Murakami, and Ault fails to teach all the elements and features of Claim 1. Accordingly, Applicant respectfully requests that the rejection of Claim 1 be withdrawn.

Dependent Claims 2-5, 8, 9 and 22

[0021] Claims 2-5, 8, 9 and 22 ultimately depend from independent Claim 1. As discussed above, Claim 1 is allowable. Therefore, Claims 2-5, 8, 9 and 22 also stand allowable for at least their dependency from an allowable base Claim 1. In addition, Carter in view of Murakami and Ault fails to teach or suggest the features of Claim 9.

Dependent Claim 9

[0022] Applicant submits that Carter in view of Murakami, and Ault fails to teach or suggest Claim 9, because Carter in view of Murakami, and Ault fails to teach, at least, the following features of Claim 9, as amended (with emphasis added):

> **determining an agent** that contains the network account credentials to be sent to the originating account

[0023] In rejecting Claim 9, the Office Action cites Ault (col. 1, line 51 to col. 2, line 20). The cited portions of Ault state:

> session manager is described as a process that is started at the same time as the Web server. Theoretically, the process runs forever, accepting requests from server processes for "proxy DCE logins" and maintaining an in-memory database of "DCE login context" information to help serve "repeated login requests" more quickly. The session manager, as envisioned in the above-identified application, must make calls to a security service to complete a proxy login. When these calls are made, memory must be allocated by the underlying DCE security code; this memory holds information associated with the DCE login context that is created. This memory is allocated within the virtual address space of the session manager process

[0024] Claim 9 recites "determining an agent that contains the network account credentials to be sent to the originating account; proxy logging on to the agent." In contrast, as discussed above, Carter a system (e.g., system 100) where a principal can

be granted with a deputy certificate "to deputize individual functions, agents, and/or other entities as deputies." Carter teacher a deputization of agent; however, Carter fails to teach "proxy logging on to the agent" as recited in Applicants amended Claim 1.

[0025] Similarly, Murakami teaches a client who wants to use a resource managed by a server, the client first requests acquisition of a token of the resource, and after the client succeeds in acquisition of the token, the client performs its job using the resource, returning the token when the use of the resource is completed. The server managing the resource ensures that the resource is not used by plurality of clients at the same time. *See col. 1, lines 59-67 of Murakami.* In other words, Murakami teaches the server managing the resource; however, Murakami fails to teach "proxy logging on to the agent" as recited in Applicants amended Claim 1.

[0026] As discussed above, Ault is directed towards enabling continuous access to Web documents stored in a secure distributed file system (Ault, col. 1, lines 9-11). Ault teaches the use of a session manager to perform a proxy login to a security service on behalf of a Web server, and ensuring persistent operation of the session manager by periodically spawning new instances of the session manager process (Ault, Abstract). Ault teaches the session manager to "make calls to a security service to complete a proxy login;" however, Ault fails to teach session manager to determine "an agent that contains the network account credentials to be sent to the originating account" as recited in Applicant's amended Claim 9.

[0027] Consequently, Carter in view of Murakami and Ault fails to teach all the elements and features of Claim 9. Accordingly, Applicant respectfully requests that the rejection of Claim 9 be withdrawn.

Dependent Claims 6-7 stand rejected under 35 U.S.C. § 103(*a*) as allegedly being anticipated by Carter in view of Murakami, Ault, and Kao

Claims 6-7

[0028] Claims 6-7 ultimately depend from independent Claim 1. As discussed above, Claim 1 is allowable. Therefore, Claims 6-7 also stand allowable for at least their dependency from an allowable base Claim 1. Accordingly, Applicant respectfully requests that the rejections for these claims be withdrawn.

New Claims 23 to 31 include features and elements that are not anticipated by Carter in view of Murakami, Ault, and Kao

Claims 23-31

[0029] Claims 23-31 include features and elements that are not taught or suggested by the cited references (i.e., Carter in view of Murakami, Ault, and Kao). Consequently, Applicant respectfully requests that the Claims 23-31 be allowed for at least these reasons.

Conclusion

[0030] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned representative for the Applicant before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Emmanuel A. Rivera/ Dated: September 15, 2009
Emmanuel A. Rivera (emmanuel@leehayes.com; 512-505 8162, ext 5001)
Registration No. 45,760

Telephone: (512) 505-8162
Facsimile: (509) 323-8979
www.leehayes.com